CONTINUATION OF APPLICATION FOR A SEARCH WARRANT

I, Aaron Eastham, being duly sworn, depose and state the following:

1. I make this Continuation in support of an application for a search warrant, authorizing investigators to examine 19 electronic devices (DEVICES) described in Attachment A, for the purpose of searching for evidence of sexual exploitation of a child (also referred to as production of child pornography), distribution or receipt of child pornography, and possession of child pornography. Child pornography is any visual depiction of a minor depicting the lascivious exhibition of the genitals or sexually explicit conduct, *see* 18 U.S.C. § 2256(8).

2. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed since 2018. I am currently assigned to the Detroit Field Office, Grand Rapids Resident Agency. During my employment with the FBI, I have conducted investigations involving violations of federal criminal laws, including violations related to child exploitation and pornography. I am familiar with the various statutes of Title 18, United States Code, Chapter 110 – sexual exploitation and other abuse of children, including violations pertaining to sexual exploitation and attempted sexual exploitation of children (18 U.S.C. § 2251(a)), distribution or receipt of child pornography (18 U.S.C.§ 2252A(a)(2)) and possession of child pornography (18 U.S.C. § 2252A(a)(5)(B)). I am a federal law enforcement officer and, therefore, authorized to request a Search Warrant under Federal Rule of Criminal Procedure 41.

3. The statements contained in this Continuation are based upon information acquired during my investigation, as well as information provided by

others such as other police officers, and Task Force Officers (TFOs) and Special Agents of the FBI. Because this Continuation is being submitted for the limited purpose of establishing probable cause to secure a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe necessary to establish probable cause to believe that there is evidence of criminal activity in violation of 18 U.S.C. §§ 2251(a), 2252A(a)(2), or 2252A(a)(5)(B) on the DEVICES (further described in Attachment A).

IDENTIFICATION OF THE DEVICES TO BE SEARCHED

4. The property to be searched consist of (1) device seized on 9/15/2021 (item a), and (18) devices seized on 9/23/2021 (items b-s).

5. The property to be searched is listed below:

a. Samsung Galaxy S10+, Black (Purple Otterbox Case), Model: SM-G975U, IMEI: 351751101791583;

b. Black Moto cellular phone (Verizon), Model XT1767, IMEI 353308080513955;

c. XBOX One Console, Model 1540, SN: 027439361848;

d. Black Amazon Tablet, Model: SX0340T;

e. Darkstar Computer Tower, white with clear blue sides;

f. LG cellular phone, Model: LG-VS425LPP, SN: 609VTTD0022393;

g. Samsung Galaxy Cellular Phone, Pink (Rose Colored Case) IMEI: 358822630986037;

h. Apple iPad (pink case), Model: A1566, SN: DLXPK13XG5VY;

i. Apple iPad (purple case), Model: A2270, SN: GG8FR9BEQ1GC;

j. HP Stream laptop, grey;

k. Toshiba Laptop, Model: Satellite C855D-S5105, SN: 2D079864Q;

l. Acer Chromebook, Model: N15Q10, SN: NXG85AA0015520B1B47600;

m. LG Cellular phone, Blue, Model: LS665, SN: 511CYZP1476629;

n. XBOX 360 S console, Model: 1439, SN: 267266602005;

o. Sony PlayStation 4 w/ Power Chord, SN: ME558166951;

p. Motorola Cellular Phone (Verizon), Model: XT1609, IMEI: 354142070947306;

q. LG Cellular Phone (Verizon), Model: LG-VS500PP, SN: 706CYBD0305349;

r. iRULU Tablet, Pink, Model: Y57; and

s. Nook Tablet, Model: BNTV600.

6. Within this Continuation, the above listed digital devices are collectively referred to as the "Devices."

7. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying and extracting the electronically stored data described in Attachment B.

PROBABLE CAUSE FOR SEARCH WARRANT

8. On or about September 15, 2021, an adult female "SR", made a report to the Allegan County Sheriff's Office regarding an incident that occurred earlier that day. SR lived in a residence hall directly above the business where BURGETT worked. The residence hall included a shared bathroom for its residents; each

resident had their own bedroom connected by a common hallway. There is a window directly above SR's bedroom door. Earlier that day, SR exited the bathroom wearing only a towel, and saw BURGETT standing in the common hallway. SR went to her bedroom, shut the door, and began changing into clothes. SR turned around and observed a camera phone being held by a hand in front of the window. The camera lens was pointed into her bedroom.

9. Police interviewed BURGETT. BURGETT admitted he was on the residence floor and did see SR coming from the bathroom to her bedroom in a towel. BURGETT further admitted that he had his cellphone in his hand while cleaning the window above SR's bedroom window. BURGETT denied taking any videos or pictures of SR but admitted that he thought about taking photographs of her.

10. Police interviewed the owners of the business located directly below the residence hall regarding BURGETT's job responsibilities. The owners of the business stated BURGETT had no responsibilities on the residence hall and should not have been in that area of the building.

11. Authorities seized BURGETT's Samsung model SM-G975U cellular phone to prevent the destruction of evidence. On or about September 16, 2021, Allegan County Sheriff's Office obtained a search warrant for BURGETT's cellular phone to search for imaged BURGETT may have taken of SR. An extraction of the cellular phone was performed using Cellebrite software. An analysis of the data extracted revealed images of child sexual abusive material (CSAM) as well as over 200 images of child pornography. The Allegan County Sheriff's Office obtained a second search warrant for BURGETT's cellular phone, to search for CSAM on the

device.

12. Some of the child pornography located on the phone's SD card included an image titled 1627999139698.jpg and depicts an adult male, anally penetrating a prepubescent female, who appears to be between 3-5 years old, and image 1627991536773.jpg that depicts a blonde-haired female, approximately 3 years of age, with an adult penis in her mouth.

13. Of the images of child pornography, several depicted what appeared to be the same prepubescent female child aged approximately 4 – 6 years' old.

14. Image file 1628300056605.jpg was located on the cellular phone's SD card. The image showed a modification date of 8/06/2021 at 9:34PM. The image depicts a clothed blonde female child, approximately 3-5 years old, next to a naked adult male with an erect penis. The adult has his hand on his penis, and the child's arm is on the adult's thigh, and her hands are near his penis. Only the bottom of the child's face was visible.

15. Image file 1601574171041.jpg is located on the cellular phone's SD card. The image shows a modification date of 10/01/2020 at 1:42PM. The image depicts a prepubescent blonde female child, holding the erect penis of what appears to be an adult male, with both hands. The child is not wearing a shirt in the photo. It is unknown if she is naked or not, because her lower body is not visible in the photo.

16. Image file 1627991584237.jpg is located on the cellular phone's SD card within the device. The image shows a modified date of 8/03/2021 at 7:53AM. The image depicts the prepubscent female child aged 4 – 6 years sleeping and a male standing over top of her masturbating. The photograph is taking from the male's

perspective.

17. During this investigation, police learned that BURGETT is a registered sex offender and resides in the Western District of Michigan with his wife and daughter, who is approximately 4 years' old.

18. On September 22, 2021, the Allegan County Sheriff's Office obtained a state search warrant for BURGETT's residence at 604 Maple Creek Drive, Holland Michigan. On September 23, 2021, Allegan County Sheriff's Deputies, assisted by FBI Agents, executed the search warrant. 18 digital devices were seized from BURGETT's residence, as well as one piece of clothing.

19. A family photo was found, on BURGETT's public facing Facebook page that appeared to be taken around Christmas time, depicting BURGETT, BURGETT's fiancé NICOLE WEERSTRA, and their child, MB (DOB:XX/2017). Officer's conducting the search claimed to have seen the photo inside the residence as well. The child in the family photo appeared to be the same child in image file 1628300056605.jpg, depicting the clothed blonde female child, next to the naked adult male with an erect penis. The background in this photo was identified to be BURGETT's bathroom.

20. BURGETT was interviewed during the execution of the search warrant and was read his Miranda Rights before he was asked any questions. During the interview BURGETT was asked if his daughter had ever touched his penis, to which BURGETT said she had. BURGETT made statements indicating that his daughter had tried to grab his penis and tried to put his penis in her mouth and BURGETT photographed the act. When asked if he was aroused during this time, he replied "I

think my penis was." He also admitted that he sent the photos he took to others, using the messaging application Kik or Whisper.

21. When BURGETT was asked about photographs of younger boys and girls engaged in sex acts, that were previously found on his phone, he made statements indicating that he received the images from others over the messaging application Kik or Whisper. BURGETT admitted to having an addicting to child pornography.

22. BURGETT's Kik account user ID is 506jonnyboy.

BACKGROUND REGARDING KIK

23. Kik Messenger, commonly called Kik, is a freeware instant messaging mobile, and available free of charge on iOS and android operating systems. It is a social networking application that permits a user to trade and disseminate various forms of digital media while using a cellular phone.

24. Kik is a free service easily downloaded as an application from the internet. Kik messenger is a feature within Kik that allows its users to communicate with selected friends as well as browse and share any website content with those whom the user selects while still within the Kik platform. Unlike other messaging apps, Kik usernames-not phone numbers-are the basis for Kik user accounts. Kik users can exchange images, videos, sketches, stickers and even web page content by posting such content privately with individual users (with whom the user selects) or publicly (on the Kik platform) with multiple individuals who belong to "groups". Groups are formed when like-minded individuals join collectively online in an online forum, created oftentimes by a Kik user designated as the Kik "Administrator" of the

group. Groups can hold up to 50 Kik usernames. Groups are created to host/discuss topics such as modern popular culture-themed ideas as well as illicit/illegal- themed ideas.

Characteristics Common among Individuals with a Sexual Interest in Children

25. Based upon my knowledge, experience, and training in child exploitation and child pornography (CP) investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals with a sexual interest in children. These common characteristics include that the individuals:

a. Generally have a sexual interest in children and receive sexual gratification from viewing children engaged in sexual activity or in sexually suggestive poses, or from literature describing such activity;

b. May collect or view sexually explicit or suggestive materials in a variety of media, including in hard copy and/or digital formats. CP viewers and collectors oftentimes use these materials for their own sexual arousal and gratification. They may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse or groom a child to participate in sexual activity, or to demonstrate desired sexual acts to a child;

c. May take photographs that either constitute CP or indicate a sexual interest in children by using cameras, video cameras, web cameras, and cellular telephones. Such images and videos may be taken with or without the child's knowledge. This type of material may be used

by the person to gratify a sexual interest in children;

d. Generally maintain their collections in a safe, secure, and private environment. These images and videos can be downloaded onto desktop or laptop computers, computer disks, disk drives, data disks, system disk operating systems, magnetic media floppy disks, Internet-capable devices, cellular telephones, tablets, digital music players, and a variety of electronic data storage devices (hardware, software, diskettes, tapes, CDs, DVDs, SD cards, memory cards, USB/jump/flash memory devices, external hard drives, and other digital storage media). Digital files and devices may be password protected, encrypted, or otherwise protected;

e. Often maintain their collections of CP and other materials indicating a sexual interest in children for a long period of time—commonly over the course of several years. These collections are also frequently maintained despite changes in residence or the acquisition of different or newer computer devices; and

f. May correspond with and/or meet others to share information and materials; rarely destroy correspondence from other CP distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, screen names, and telephone numbers of individuals with whom they have been in contact and who share the same interests in CP. Such correspondence may take place, for example, through online bulletin boards and forums, Internet-based chat messaging, email, text message,

video streaming, letters, telephone, and in person. In some cases, these individuals may have joint involvement in CP activities with others within their household or with whom they share a close relationship (e.g., brothers/siblings dating partners, or coworkers).

Specifics of Seizing and Searching Computer Systems

26. Computers and Internet-capable devices such as tablets and cellular telephones facilitate access to messaging applications, which can be used to locate and communicate with minors online for the purposes of enticement or other adults who share an interesting in child pornography who send or trade child pornography. The Internet affords various platforms, through messaging applications, forums, websites, and social media, to connect with individuals, including minors, across the world, in a relatively secure and anonymous fashion.

27. Storage capacity of computers and portable storage media, such as USB or thumb drives, has grown tremendously within the last several years. These drives can store thousands of images at very high resolution, are easily transportable, and are relatively inexpensive. Advances in technology have significantly reduced the size of digital storage devices such that now large numbers of digital files can be stored on media that will fit in a person's pocket, on a keychain, or in any number of easily transportable and concealable places. An individual can now easily carry on his or her person storage media that contains thousands of files, including images, chat logs, video files, and full-length movie files.

28. As with most digital technology, communications made from a computer device are often saved or stored on that device. Storing this information can be

intentional, for example, by saving an email as a file on the computer or saving the location as a "favorite" website in a "bookmarked" file. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be stored automatically in many places, such as temporary files or Internet Service Provider (ISP) client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files.

29. A forensic examiner often can recover evidence that shows whether a computer device contains peer-to-peer software, when the device was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space—for long periods of time before they are overwritten.

30. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are

only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

31. Searches and seizures of evidence from computers and computer devices commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices can store the equivalent of millions of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert

should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

32. In order to retrieve data fully from a computer system, the analyst needs all storage devices as well as the central processing unit. In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

33. Forensic examiners can also find the presence or absence of certain software and programs to determine who controlled a computer at a given time. Such evidence includes: viruses, Trojan horses, spyware, malware, and other forms of malicious software; the presence or absence of security software designed to detect malicious software; the lack of malicious software; and the presence or absence of software designed to protect a device from infiltration, access, or control by another person or entity, which may include pop-up blockers, security software, password

protection, and encryption. Forensic examiners can also find evidence of software or programs designed to hide or destroy evidence.

34. The time period required for a complete, safe, and secure forensic examination of the computer and storage media is uncertain. The government will make available for pick-up within a reasonable time all items found not to contain any contraband or material to be seized pursuant to the warrant and all hardware and software no longer needed for examination purposes. In conducting the search, the forensic examiner and agents will examine files regardless of their name because such names and file extensions can be altered to conceal their actual content. Because of the volume of data to be searched and the need to complete the examination in a reasonable time, the forensic examiner will also use computer techniques such as keyword searches that may result in the display of irrelevant materials.

35. Retention of any computers would be warranted, if any CP is found thereon, in order to permit forfeiture of those computers and related properties as instrumentalities of the crime, pursuant to 18 U.S.C. §§ 2253(a)(3) and 2254(a)(2).

36. I am aware that the recovery of data by a computer forensic analyst takes significant time. For this reason, the Return inventory will contain a list of the tangible items being examined. Unless otherwise ordered by the Court, the Return will not include evidence later examined by a forensic analyst.

CONCLUSION

37. Based upon the above information, I respectfully submit there is probable cause to for a search warrant authorizing the examination of the Devices

described in Attachment A to seek the information described in Attachment B.